UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
MIDLAND/ODESSA DIVISION

Malikie Innovations Ltd. and
Key Patent Innovations Ltd.,

Plaintiffs,

v.

MARA Holdings, Inc. (f/k/a Marathon Digital Holdings, Inc.)

Defendant.

Case No. 7:25-cv-00222- DC-DTG

DEFENDANT'S MOTION TO DISMISS UNDER RULE 12(B)(6)

TABLE OF CONTENTS

I. Introduction 1
II. Background 2
A. The ’286 Patent and Montgomery Reductions 2
B. Malikie’s Infringement Allegations 5
III. Legal Standards 7
IV. Argument 7
A. The Reduction Value Limitation Is Material to Practicing the Asserted Claim 8
B. The Complaint Fails to Plead Infringement of the Reduction Value Limitation .. 10
V. Conclusion 12

TABLE OF AUTHORITIES

Cases

Ashcroft v. Iqbal,
556 U.S. 662 (2009) 1, 7

Bot M8 LLC v. Sony Corporation of America,
4 F.4th 1342 (Fed. Cir. 2021) 7, 11

Disc Disease Sols. Inc. v. VGH Sols., Inc.,
888 F.3d 1256 (Fed. Cir. 2018) 7

Vervain, LLC v. Micron Tech., Inc.,
No. 6:21-CV-00487-ADA, 2022 WL 23469 (W.D. Tex. Jan. 3, 2022) ..... passim

I. INTRODUCTION

The Sixth Claim in Plaintiffs Malikie Innovations Ltd.'s and Key Patent Innovations Ltd.'s ("Malikie's) Complaint—alleging infringement of U.S. Patent No. 8,532,286—should be dismissed for failure to state a claim. *See Ashcroft v. Iqbal*, 556 U.S. 662 (2009). Malikie's threadbare allegations of infringement fail to meet the pleading standard for the same reasons this Court articulated in *Vervain, LLC v. Micron Tech., Inc.*, No. 6:21-CV-00487-ADA, 2022 WL 23469, at *5 (W.D. Tex. Jan. 3, 2022) (Albright, J.).

First, "a higher level of detail in pleading infringement may—depending on the complexity of the technology—be demanded for elements clearly 'material' to novelty and non-obviousness." *Micron*, at *5. For the '286 patent, the specification and prosecution history confirm that the alleged point of novelty of the claimed invention is limitation 1[b] (hereinafter, the "Reduction Value Limitation"). Specifically, the patent describes an admitted prior art algorithm (Fig. 4) and a modified algorithm (Fig. 7), both of which involve the same input, the same output, iterations, and zeroing the least significant word at each iteration. The only difference is the use of a "modified reduction value" *n'*. As reflected in the prosecution history and on the face of claim 1, the only possible difference between claim 1 and the admitted prior art is the Reduction Value Limitation.

Second, "[i]n cases involving complex technology, a complaint nakedly alleging that the accused product practices the claimed invention's point of novelty will rarely suffice." *Micron*, at *5. The claim chart attached to the Complaint merely parrots the claim language and provides a basic narrative accompanied by excerpts of open source Bitcoin Core code, relating only to limitations 1[a] ("obtaining an operand") and 1[c] ("outputting the modified operand"), which are merely aspects of the admitted prior art. Not only does the claim chart fail to even identify a reduction value, it entirely fails to articulate how the Reduction Value Limitation is infringed.

Indeed, Malikie fails to plead any logical connection between the excerpted code and the Reduction Value Limitation.

There is no excuse for Malikie's inadequate pleading. The infringement claim for the '286 patent targets ***publicly available, open source code files*** (i.e., Bitcoin Core). *See* Compl., Ex. 12 at 5 (citing Bitcoin Core's public GitHub webpage), 6-7 (same). Malikie cannot sustain an infringement claim by "merely articulating why it is plausible that the accused product practices the prior art." *Id*. at *5. For these reasons, as more fully set forth below, Malikie's claim for infringement of the '286 patent should be dismissed.

II. BACKGROUND

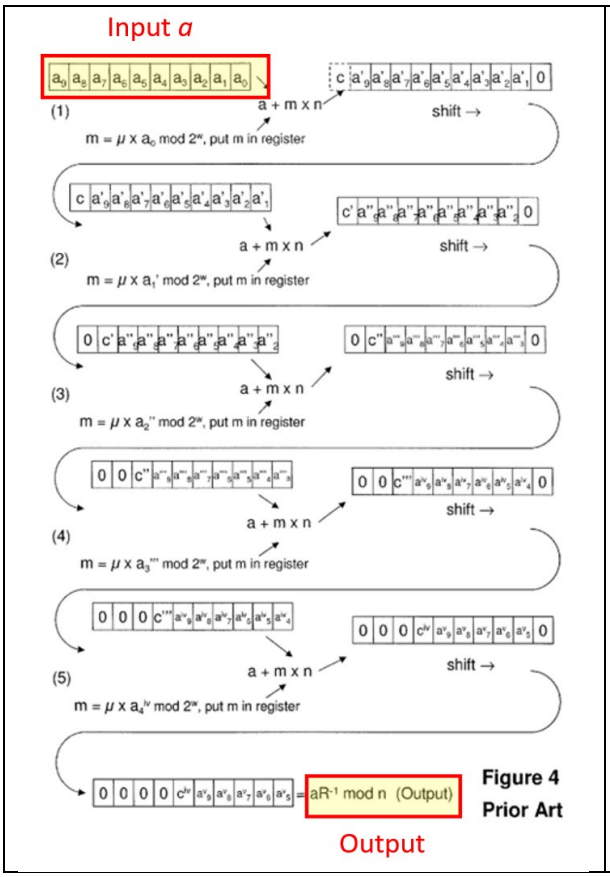
A. The '286 Patent and Montgomery Reductions

The '286 patent describes an algorithm for performing a "Montgomery-style reduction." Montgomery modular reduction, or Montgomery reduction for short, refers to mathematical algorithms for performing modular arithmetic while avoiding computationally expensive division operations. '286 patent at 1:20-36. Modular arithmetic refers to operations such as addition, subtraction, and multiplication *modulo*[1] some number. "The calculation of the remainder is referred to as reduction in modular arithmetic." *Id.* Per the '286 patent, "the step of calculating the remainder is considered slow," and the "most commonly used" method for modular reduction is Montgomery reduction. *Id.* "Montgomery reduction avoids the expensive division operations typically used in classical modular reduction." *Id.* The output of a Montgomery reduction is

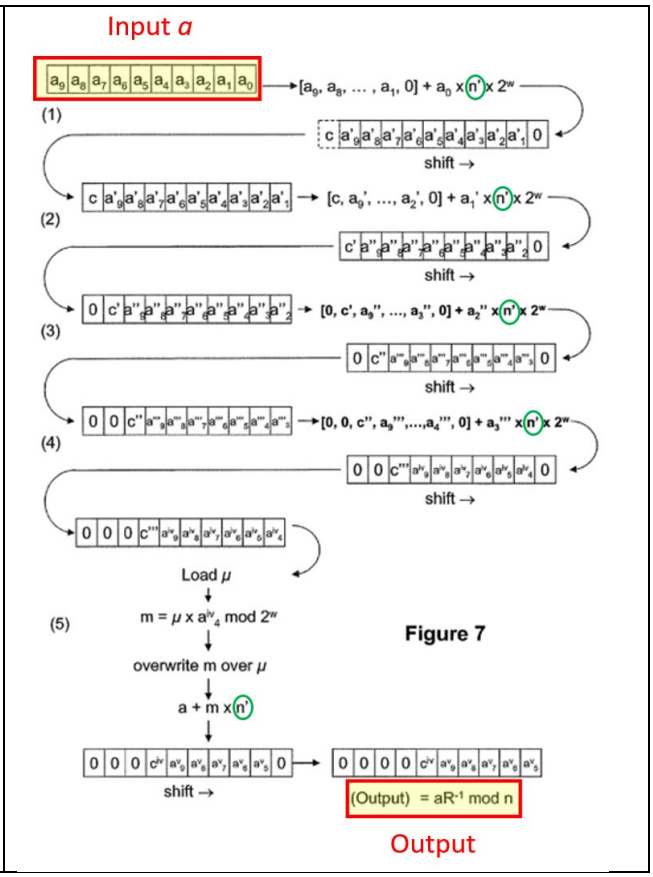
[1] A modulo or "mod" operation calculates the remainder after one number is divided by another, the latter number being called the "modulus" of the operation. For example, $5 \; mod \; 2 = 1$ because a remainder of 1 is left over after dividing 5 by 2.

referred to in the patent as the "Montgomery form," which is written as $aR^{-1} mod\ n$ for a value a reduced modulo n.[2]

The '286 patent describes two algorithms for performing a Montgomery reduction: (i) a "typical" or "prior art" algorithm and (ii) a "modified Montgomery reduction using [a] modified reduction value," which is the purported invention. *See* '286 patent at 3:1-17, Figs. 3-7. Figure 4 (prior art algorithm) and Figure 7 (modified algorithm), copied below and annotated, illustrate the similarities of the two algorithms.

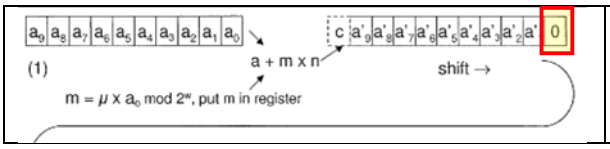


'286 patent at Fig. 4 (annotated)

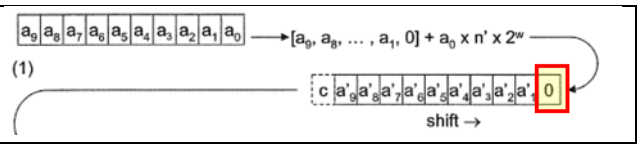


'286 patent at Fig. 7 (annotated)

[2] Per the '286 patent, the value R is an auxiliary number called the "radix" or "base," and it can be chosen. '286 patent at 1:47-52.



'286 patent at Fig. 4 (annotated)



'286 patent at Fig. 7 (annotated)

As shown above, in both the prior art algorithm (Fig. 4) and "new" algorithm (Fig. 7):

1. A value *a* is the input;

2. The output is the Montgomery form $aR^{-1} mod\ n$;

3. The value *a* is reduced iteratively (five iterations in the example); and

4. At each iteration, the least-significant "word"[3] of *a* becomes "zeroed." *See also* '286 patent at 5:8-10 ("In the result, the least significant word a_0 is 'zeroed' . . . "), 6:32-35 ("As shown in FIG. 7 … at each iteration, the least significant word of a is zeroed . . .").

The difference between the admitted prior art algorithm (Fig. 4) and the modified algorithm (Fig. 7) is in the steps performed at each iteration. Specifically, the '286 patent describes the use of a "modified reduction value" *n'* (circled in green in Fig. 7 above). The '286 patent discloses a single formula for the modified reduction value: $\boldsymbol{n' = 2^{-w} mod\ n}$. '286 patent at 5:45-49. As described in the patent, the reduction value *n'* has the "useful" property that $1 \equiv n' * 2^w$. *See* '286 patent at Fig. 5.

> To see the usefulness of this new value, it is noted that if the value n' is then shifted up by one digit, which is equivalent to multiplying by 2^w, a value is obtained that is equivalent to 1 mod n. **Consequently, the value a_0 can be replaced** with $a_0$xn'x2^w, that is, a_0 multiplied by n' shifted up one digit.

'286 patent at 5:56-60 (emphasis added).

Claim 1 of the '286 patent, which is the only allegedly infringed claim identified in the Complaint, is reproduced below with the Reduction Value Limitation in bold.

[3] A "word" or "computer word" refers to the "wordsize of the machine in bits." '286 patent at 2:21-23. A 32-bit computer, for example, may have 32-bit "words."

> [1Pre] 1. A method for performing, on a cryptographic apparatus, a Montgomery-style reduction in a cryptographic operation, the method comprising:
>
> [1a] obtaining an operand for the cryptographic operation;
>
> **[1b] computing a modified operand using a reduction value, instead of a modulus used in performing a standard Montgomery reduction, to perform a replacement of a least significant word of the operand, rather than perform a cancellation thereof, the reduction value being a function of the modulus; and**
>
> [1c] outputting the modified operand.

B. Malikie's Infringement Allegations

The Complaint alleges infringement of claim 1 of the '286 patent under 35 U.S.C. § 271(a) based on MARA's alleged use of "hardware and/or software . . . that comply with the Bitcoin protocol." Compl. ¶ 146. Exhibit 12 to the Complaint, which is referenced in ¶ 146, contains an infringement claim chart for claim 1 of the '286 patent.

The claim chart is divided into two rows of evidence: a first row for the preamble and a second row for the rest of the claim (i.e., limitations [1a], [1b], and [1c]). The second row is reproduced below, and includes allegations by Malikie (highlighted in yellow) and three excerpts from Bitcoin Core source code header files scalar.h and scalar_4x64_impl.h with some of the code in bold.

[1a] obtaining an operand for the cryptographic operation;	MARA obtains an operand for the cryptographic operation; computes a modified operand using a reduction value, instead of a modulus used in performing a standard Montgomery reduction, to perform a replacement of a least significant word of the operand, rather than perform a cancellation thereof, the reduction value being a function of the modulus; and outputs the modified operand. *See, e.g.*:

[1b] computing a modified operand using a reduction value, instead of a modulus used in performing a standard Montgomery reduction, to perform a replacement of a least significant word of the operand, rather than perform a cancellation thereof, the reduction value being a function of the modulus; and
 	
[1c] outputting the modified operand.
	For example, operand `l` is 8 machine words, reduced operand `r` is 4 machine words. *See, e.g.*:
	
	`/** Set a scalar to an unsigned integer. */`
	`static void secp256k1_scalar_set_int(secp256k1_scalar *r, unsigned int v);`
	See, e.g., src/secp256k1/src/scalar.h
	
	`/* Limbs of the secp256k1 order. */`
	`#define SECP256K1_N_0 ((uint64_t)0xBFD25E8CD0364141ULL)`
	`#define SECP256K1_N_1 ((uint64_t)0xBAAEDCE6AF48A03BULL)`
	`#define SECP256K1_N_2 ((uint64_t)0xFFFFFFFFFFFFFFFEULL)`
	`#define SECP256K1_N_3 ((uint64_t)0xFFFFFFFFFFFFFFFFULL)`
	
	`/* Limbs of 2^256 minus the secp256k1 order. */`
	`#define SECP256K1_N_C_0 (~SECP256K1_N_0 + 1)`
	`#define SECP256K1_N_C_1 (~SECP256K1_N_1)`
	`#define SECP256K1_N_C_2 (1)`
	
	`SECP256K1_INLINE static void secp256k1_scalar_set_int(secp256k1_scalar *r, unsigned int v) {`
	`  r->d[0] = v;`
	`  r->d[1] = 0;`
	`  r->d[2] = 0;`
	`  r->d[3] = 0;`
	`  ...;`
	`}`
	
	`static void secp256k1_scalar_mul(secp256k1_scalar *r, const secp256k1_scalar *a, const secp256k1_scalar *b) {`
	`  uint64_t l[8];`
	`  ...;`
	`  secp256k1_scalar_mul_512(l, a, b);`
	`  secp256k1_scalar_reduce_512(r, l);`
	`  ...;`
	`}`
	
	See, e.g., src/secp256k1/src/scalar_4x64_impl.h (*see also* code in "scalar_8x32_impl.h")

	For example, operand `l` is reduced until it fits in p[0..4], which is further reduced into `r`. *See, e.g.*:
	
	`SECP256K1_INLINE static int secp256k1_scalar_reduce_512(secp256k1_scalar *r, const uint64_t *l) {`
	`  secp256k1_uint128 c128;`
	`  ...;`
	`  uint64_t n0 = l[4], n1 = l[5], n2 = l[6], n3 = l[7];`
	`  ...;`
	`  /* Reduce 512 bits into 385. */`
	`  /* m[0..6] = l[0..3] + n[0..3] * SECP256K1_N_C. */`
	`  ...;`
	`  /* Reduce 385 bits into 258. */`
	`  /* p[0..4] = m[0..3] + m[4..6] * SECP256K1_N_C. */`
	`  ...;`
	`  /* Reduce 258 bits into 256. */`
	`  /* r[0..3] = p[0..3] + p[4] * SECP256K1_N_C. */`
	`  secp256k1_u128_from_u64(&c128, p0);`
	`  secp256k1_u128_accum_mul(&c128, SECP256K1_N_C_0, p4);`
	`  r->d[0] = secp256k1_u128_to_u64(&c128); ...;`
	`}`
	
	See, e.g., src/secp256k1/src/scalar_4x64_impl.h (*see also* code in "scalar_8x32_impl.h")

Compl., Ex. 12 at 7–9

III. LEGAL STANDARDS

To state a claim for direct infringement, the plaintiff must plead "factual content" which creates a "reasonable inference" that the accused products meet "each and every element of at least one claim" of the asserted patent. *Disc Disease Sols. Inc. v. VGH Sols., Inc.*, 888 F.3d 1256, 1260 (Fed. Cir. 2018) (quoting *Iqbal*, 556 U.S. at 678).

"The degree of detail required to sufficiently plead direct infringement depends on 'the complexity of the technology, the materiality of any given element to practicing the asserted claim(s), and the nature of the allegedly infringing device.'" *Micron*, at *5 (quoting *Bot M8 LLC v. Sony Corporation of America*, 4 F.4th 1342, 1353 (Fed. Cir. 2021)). "Under any standard, however, the complaint must support its entitlement to relief with 'factual content,' not just conclusory allegations that the accused product(s) meet every claim limitation." *Id.* at *2. Providing a claim chart with "element-by-element mapping" is not alone sufficient, rather "[t]he Court must consider whether the factual allegations therein, 'when taken as true, articulate why it is plausible that the accused product infringes the patent claim." *Id*. at *7; *see also Bot M8*, 4 F.4th at 1354 ("[I]t is the *quality* of the allegations, not the *quantity*, that matters.").

IV. ARGUMENT

The Complaint utterly fails to articulate why it is plausible that MARA practices the Reduction Value Limitation 1[b] of claim 1 of the '286 patent. The level of detail provided in the Complaint does not meet the standard demanded of the Reduction Value Limitation 1[b], which is material to practicing the asserted claim and in fact contains the only alleged point of novelty over the admitted prior art. Despite its materiality, the Reduction Value Limitation is the only limitation for which Malikie has provided no allegations as to how MARA purportedly infringes. Instead, Malikie's claim chart merely parrots the claim language and provides excerpts of open source code

files that bear no resemblance to the Reduction Value Limitation, and at most, show that MARA may perform steps from the admitted prior art.

The Sixth Claim of the Complaint should be dismissed because Malikie has failed to plausibly allege infringement of the '286 patent.

A. The Reduction Value Limitation Is Material to Practicing the Asserted Claim

The specification and prosecution history confirm that the Reduction Value Limitation is the alleged point of novelty for claim 1 of the '286 patent. Accordingly, the Reduction Value Limitation is "material to practicing the asserted claim." *Micron*, at *5.

First, as discussed above in Section II.A, the specification shows that the admitted prior art Montgomery reduction algorithm (Fig. 4) is substantially similar to the purported invention (Fig. 7). The sole difference is in the use of a particular "reduction value." *See also* Compl. ¶ 109 (describing the use of a particular "reduction value" as the "inventive technique").

Second, the prosecution history confirms that the Reduction Value Limitation "lays at the point of novelty."[4] The applicant distinguished claim 1 over prior art based on the Reduction Value Limitation. Ex. 1 (October 10, 2012 Applicant Remarks) at 11 ("Sabin may teach details of a Montgomery Reduction, however, Sabin does not teach or fairly suggest the use of a modified reduction value, let alone as recited in claim 1."); Ex. 2 (May 1, 2013 Applicant Remarks) at 7 ("A modified process cannot be considered equivalent to a reduction value unless the process is modified using such a value."); *id.* at 7 ("[N]ot only is the claimed method used to perform a reduction differently, a reduction value is used, as clearly recited in claim 1."); Ex. 3 (May 13, 2013 Notice of Allowance) at 2 ("[T]he prior art fails to teach or reasonably suggest the invention

[4] The Court may take judicial notice of the prosecution history of the '286 patent. *Micron*, at *5 & n.2.

as claimed. For example, see the applicant's remarks filed on 5/1/13, which contrasts the cited references against the invention as claimed.").

The applicant made two claim amendments during prosecution of the '286 patent, both to limitation [1b], and both to distinguish the claim over prior art rejections:

Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of claims:

1. (currently amended) A method for performing on a cryptographic apparatus a Montgomery-style reduction in a cryptographic operation, the method comprising:

obtaining a modified reduction value, the modified reduction value being a function of a modulus used in performing a standard Montgomery reduction;

computing a modified operand by applying the modified reduction value, instead of the modulus, to perform a replacement of a least significant word of the operand, rather than perform a cancellation thereof; and

outputting the modified operand.

Ex. 1 (October 10, 2012 Applicant Remarks) at 4

Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of claims:

1. (currently amended) A method for performing, on a cryptographic apparatus, a Montgomery-style reduction in a cryptographic operation, the method comprising:

obtaining an operand for the cryptographic operation ~~a modified reduction value, the modified reduction value being a function of a modulus used in performing a standard Montgomery reduction~~;

computing a modified operand ~~by applying the~~ using a ~~modified~~ reduction value, instead of [[the]] a modulus used in performing a standard Montgomery reduction, to perform a replacement of a least significant word of the operand, rather than perform a cancellation thereof, the reduction value being a function of the modulus; and

outputting the modified operand.

Ex. 2 (May 1, 2013 Applicant Remarks) at 2

Thus, based on statements made during prosecution, in the Complaint, and in the patent itself, the Reduction Value Limitation is material to practicing the asserted claims.

B. The Complaint Fails to Plead Infringement of the Reduction Value Limitation

The level of detail provided in the Complaint does not meet the pleading standard here, "where the technology is not simple and the limitations-at-issue are material." *Micron*, at *5.

First, the narrative statements by Malikie in the claim chart attached to the Complaint do not explain how the accused products could plausibly infringe the Reduction Value Limitation 1[b]. As shown in Section II.B above, the claim chart contains three narrative statements for limitations [1a]–[1c]:

> MARA obtains an operand for the cryptographic operation; computes a modified operand using a reduction value, instead of a modulus used in performing a standard Montgomery reduction, to perform a replacement of a least significant word of the operand, rather than perform a cancellation thereof, the reduction value being a function of the modulus; and outputs the modified operand.
> . . .
> For example, operand l is 8 machine words, reduced operand r is 4 machine words.
> . . .
> For example, operand l is reduced until it fits in p[0..4], which is further reduced into r.

Compl., Ex. 12 at 7–9. The first statement is conclusory and "merely track[s] the claim language." *Micron*, at *7. The second and third statement, at most, address limitations [1a] ("obtaining an **operand** for the cryptographic operation") and [1c] ("outputting the **modified operand**"). For limitation [1b] (the Reduction Value Limitation), Malikie provides no explanation.

Second, the claim chart includes three block excerpts to open source Bitcoin Core code with some code in bold, but Malikie does not plead a logical connection between the code and the Reduction Value Limitation [1b]. None of the excerpted code bears any resemblance to the

modified reduction value described and claimed in the '286 patent, and for all three excerpts, the relevance of the bold code is unclear and unexplained.

Moreover, even assuming in the absence of any explanation, that Malikie is alleging infringement based on the function "secp256k1_scalar_reduce_512" purportedly reducing, in iterations, the "operand l" into the "reduced operand r," this is plainly insufficient to state a claim for infringement.

```
SECP256K1_INLINE static int secp256k1_scalar_reduce_512(secp256k1_scalar *r, const
uint64_t *l) {
    secp256k1_uint128 c128;
    ...;
    uint64_t n0 = l[4], n1 = l[5], n2 = l[6], n3 = l[7];
    ...;
    /* Reduce 512 bits into 385. */
    /* m[0..6] = l[0..3] + n[0..3] * SECP256K1_N_C. */
    ...;
    /* Reduce 385 bits into 258. */
    /* p[0..4] = m[0..3] + m[4..6] * SECP256K1_N_C. */
    ...;
    /* Reduce 258 bits into 256. */
    /* r[0..3] = p[0..3] + p[4] * SECP256K1_N_C. */
    secp256k1_u128_from_u64(&c128, p0);
    secp256k1_u128_accum_mul(&c128, SECP256K1_N_C_0, p4);
    r->d[0] = secp256k1_u128_to_u64(&c128); ...;
}
```

See, e.g., src/secp256k1/src/scalar_4x64_impl.h (*see also* code in "scalar_8x32_impl.h")

Compl., Ex. 12 at 9

As explained in Section II.A, the admitted prior art discloses reducing, in iterations, an operand into a reduced operand. As this Court has recognized, "a plaintiff cannot establish 'why it is plausible that the accused product infringes the patent claim' by merely articulating why it is plausible that the accused product practices the prior art." *Micron*, at *5 (quoting *Bot M8*, 4 F.4th at 1353) (internal citations omitted).

Here, Malikie does not identify the actual reduction algorithm in Bitcoin Core, which as noted above is publicly available, or make any plausible allegations as to why the actual reduction

algorithm is performed the particular way of the '286 patent (that is purportedly different from the admitted prior art), i.e., "computing a modified operand using a reduction value, instead of a modulus used in performing a standard Montgomery reduction, to perform a replacement of a least significant word of the operand, rather than perform a cancellation thereof, the reduction value being a function of the modulus." '286 patent at 9:27-32 (Claim 1).

"In cases involving complex technology, a complaint nakedly alleging that the accused product practices the claimed invention's point of novelty will rarely suffice." *Micron*, at *5. At best, Malikie has merely plead that MARA is practicing the admitted prior art, which is insufficient to plausibly state a claim for infringement of the '286 patent.

V. CONCLUSION

Malikie has failed to plausibly allege infringement of the '286 patent. Accordingly, MARA respectfully requests that the Court dismiss the Sixth Claim of the Complaint.

Dated: July 21, 2025

Respectfully Submitted,

By: */s/ Steve Wingard*
Steve Wingard
State Bar No. 00788694
swingard@scottdoug.com
Stephen L. Burbank
State Bar No. 24109672
sburbank@scottdoug.com
Robert P. Earle
State Bar No. 241245566
rearle@scottdoug.com
Scott Douglass & McConnico LLP
303 Colorado Street, Suite 2400
Austin, TX 78701-3234
Telephone: (512) 495-6300
Facsimile: (512) 495-6399

Anish R. Desai
Elizabeth S. Weiswasser
Ian A. Moore
Tom Yu
Thomas Macchio
Paul, Weiss, Rifkind, Wharton & Garrison LLP
1285 Sixth Avenue
New York, NY 10019
Telephone: (212) 373-3000

Christopher M. Pepe
W. Sutton Ansley
Eric C. Westerhold
Paul, Weiss, Rifkind, Wharton & Garrison LLP
2001 K Street NW
Washington, DC 20006
Telephone: (202) 223-7300

Counsel for Defendant MARA Holdings, Inc.

CERTIFICATE OF SERVICE

I hereby certify that I have served a true and correct copy of this motion upon each attorney of record and the original upon the Clerk of Court on this the 21st day of July, 2025.

/s/ Steve Wingard
Steve Wingard